**International Journal of Research in Advanced Engineering and Technology**
**ISSN: 2455-0876**
**Impact Factor: RJIF 5.44**
**www.newengineeringjournal.in**
**Volume 4; Issue 1; January 2018; Page No. 01-08**

# Cloud computing and cloud security

**[1] Amit Kumar Nahar, [2] Kanika Mongia, [3] Sarla Kumari**
[1] MCA, NIT Agartala, Tripura, India
[2] Assistant Professor, Dept. of Computer, N.B.G.S.M. College, Sohna, Gurugram, Haryana, India
[3] MCA, IGPGRC, Mirpur, Rewari, Haryana, India.

**Abstract**
Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce. Som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

**Keywords:** security issues, cloud security, cloud architecture, data protection, cloud platform, grid computing

## Introduction

**Why we used cloud computing**

1. Flexibility
2. Disaster recovery
3. Work from anywhere
4. Automatic software updates
5. Document control
6. Security
7. Environmental friendly
8. Backup
9. File storage

**Cloud computing is a general term for the delivery of hosted services over the internet.**

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers Cloud computing appeared as a business necessity, being animated by the idea of just using the infrastructure without managing it. Although initially this idea was present only in the academic area, recently, it was transposed into industry by companies like Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new startups to enter the market easier, since the cost of the infrastructure is greatly diminished. This allows developers to concentrate on the business value rather on the starting budget. The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs.

Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business

applications which are accessed from servers through web browers.

**Objectives of the study**

1. Coping with the Physical
2. Securing Data on the Network
3. Dealing with Threats
4. Confidentiality
5. Integrity
6. Availability

**Research Methodology**

- The descriptive methodology has been use to collect data
- Secondary data has been collected from various published source and website
- The explanation of data is more qualitative than on quantitative term

**Overview of cloud computing and cloud security**

Cloud computing is a big shift from the traditional way businesses think about IT resources. What is it about cloud computing? Why is cloud computing so popular? Here are 6 common reasons organizations are turning to cloud computing services:

**1. Cost**

Cloud computing eliminates the capital expense of buying hardware and software and setting up and running on-site datacenters—the racks of servers, the round-the-clock electricity for power and cooling, the IT experts for managing the infrastructure. It adds up fast.

**2. Speed**

Most cloud computing services are provided self service and on demand, so even vast amounts of computing resources can be provisioned in minutes, typically with just a few mouse clicks, giving businesses a lot of flexibility and taking the pressure off capacity planning.

**3. Global Scale**

The benefits of cloud computing services include the ability to scale elastically. In cloud speak, that means delivering the right amount of IT resources—for example, more or less computing power, storage, bandwidth—right when its needed and from the right geographic location.

**4. Productivity**

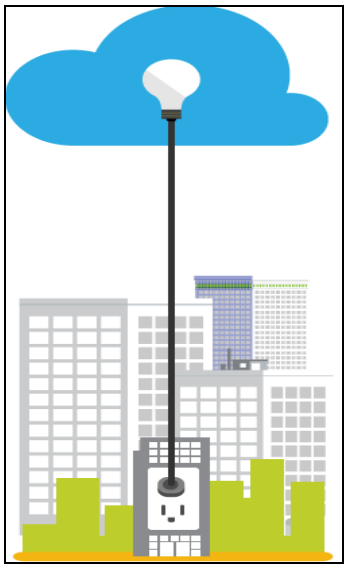
On-site datacenters typically require a lot of "racking and stacking"—hardware set up, software patching and other time-consuming IT management chores. Cloud computing removes the need for many of these tasks, so IT teams can spend time on achieving more important business goals.

**5. Performance**

The biggest cloud computing services run on a worldwide network of secure datacenters, which are regularly upgraded to the latest generation of fast and efficient computing hardware. This offers several benefits over a single corporate datacenter, including reduced network latency for applications and greater economies of scale.

**6. Reliability**

Cloud computing makes data backup, disaster recovery and business continuity easier and less expensive, because data can be mirrored at multiple redundant sites on the cloud provider's network.



**Types of cloud services**

IaaS, PaaS, SaaS

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a

service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another. Knowing what they are and how they are different makes it easier to accomplish your business goals.

**Infrastructure-as-a-service (IaaS)**
The most basic category of cloud computing services. With IaaS, you rent IT infrastructure servers and virtual machines (VMs), storage, networks, operating systems from a cloud provider on a pay-as-you-go basis.

**Platform as a service (PaaS)**
Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

**Software as a service (SaaS)**
Software-as-a-service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

**Types of cloud deployments**
Public, private, hybrid
Not all clouds are the same. There are three different ways to deploy cloud computing resources: public cloud, private cloud and hybrid cloud.

**Public cloud**
Public clouds are owned and operated by a third-party cloud service provider, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

**Private cloud**
A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

**Hybrid Cloud**
Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options

**Cloud computing entities**
Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows.

**Cloud Providers**
Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centers) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers.

**Cloud Service Brokers**
Includes technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

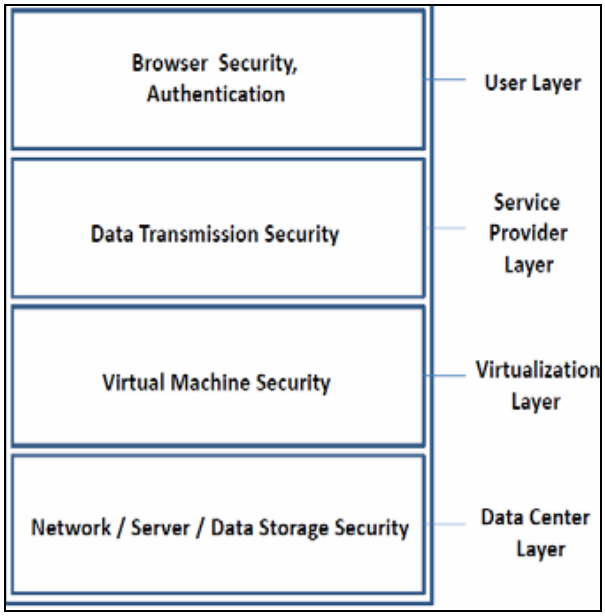
**Cloud Resellers**
Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region. Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller. In the next section, key benefits of and possible threats and risks for Cloud Computing are listed.

**Cloud computing security architecture**
Security within cloud computing is an especially worrisome

issue because of the fact that the devices used to provide services do not belong to the users themselves. The users have no control of, nor any knowledge of, what could happen to their data. This is a great concern in cases when users have valuable and personal information stored in a cloud computing service. Users will not compromise their privacy so cloud computing service providers must ensure that the customers' information is safe. This, however, is becoming increasingly challenging because as security developments are made, there always seems to be someone to figure out a way to disable the security and take advantage of user information. Some of the important components of Service Provider Layer are SLA Monitor, Metering, Accounting, Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management. Some of the security issues related to Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity and Binding Issues. Some of the important components of Virtual Machine Layer creates number of virtual machines and number of operating systems and its monitoring. Some of the security issues related to Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity issues, Identity and Access management Some of the important components of Data Center (Infrastructure) Layer contains the Servers, CPU's, memory, and storage, and is henceforth typically denoted as Infrastructure-as-a-Service (IaaS). Some of the security issues related to Data Center Layer are secure data at rest, Physical Security: Network and Server.

Some organizations have been focusing on security issues in the cloud computing. The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Open Security Architecture (OSA) is another organizations focusing on security issues. They propose the OSA pattern, which pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis. For example, the Certification, Accreditation, and Security Assessments series increase in importance to ensure oversight and assurance given that the operations are being "outsourced" to another provider. System and Services Acquisition is crucial to ensure that acquisition of services is managed correctly. Contingency planning helps to ensure a clear understanding of how to respond in the event of interruptions to service delivery [8]. The Risk Assessment controls are important to understand the risks associated with services in a business context. National Institute of Standard and Technology (NIST), USA (http://www.nist.gov/) has initiated activities to promote standards for cloud computing [15]. To address the challenges and to enable cloud computing, several standards groups and industry consortia are developing Specifications and test beds. Some of the existing standards and test bed groups are Cloud Security Alliance (CSA), Internet Engineering Task Force (IETF), storage Networking Industry Association (SNIA) etc. On the other side, a cloud API provides either a functional interface or a management interface (or both). Cloud management has multiple aspects that can be standardized for interoperability. Some possible standards are Federated security (e.g., identity) across clouds, Metadata and data exchanges among clouds, Standardized outputs for monitoring, auditing, billing, reports and notification for cloud applications and services, Cloud-independent representation for policies and governance etc.

Figure




High Level Security Architecture of Cloud Computing

**Key Security Issues In Cloud Computing**

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location

- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

**Access to servers & applications**

In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which is not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. Some organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users.

Most companies are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of SMB companies, a segment that has the highest cloud application adoption rate, Active Directory (AD) seems to be the most popular tool for managing users. With cloud application, the software is hosted outside of the corporate firewall. Many times user credentials are stored in the cloud application Providers databases and not as part of the corporate IT infrastructure. This means SaaS customers must remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple cloud application products will increase IT management overhead. For example, cloud application providers can provide delegate the authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users. Large enterprises, the management of user's account as the adoption of single sign on (SSO) or each employee will be dispatched some different accounts to access different systems. Thus, multi-authentication for each employee might be very often to be confronted in an enterprise. Those accounts that come along with each individuals might be the same or different. Therefore, how could the administrator well manage those user's identification accounts and the corresponding passwords or achieve the state of SSO is another important issue. Nevertheless, the application of SSO for identification and authentication does have serious information security risk. In addition, the management of authorized access privilege is also a critical key point.

**Data Transmission**

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

**Virtual machine security**

Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in para-virtualization, an operating system is modified so that it can be run concurrently with other operating systems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices such as I/O devices, storage, memory, etc. Many bugs have been found in all popular VMMs that allow escaping from Virtual machine. Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability was found in VMware's shared folders mechanism that grants users of a guest system read and write access to any portion of the host's file system including the system folder and other security-sensitive files. Vulnerability in Xen can be exploited by "root" users of a guest domain to execute arbitrary commands. The other issue is the control of administrator on host and guest operating systems. Current VMMs (Virtual Machine Monitor) do not offer perfect isolation. Virtual machine monitor should be 'root secure', meaning that no privilege within the virtualized guest environment permits interference with the host system.

**Network Security**

Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems.

Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network.

Reused IP address issue have been a big network security concern. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user.

**Data Security**

For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party.

**Data Privacy**

The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks.

**Data Integrity**

Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

**Data Location**

In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications.

In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the

distributed system should be able to participate in the global transaction via a resource manager.

**Data Availability**

Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.

**Data Segregation**

Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

**Security Policy and Compliance**

Traditional service providers are subjected to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it leads to a obvious decrease in customer trust. Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as PCI, HIPAA, and GLBA in addition to auditing practices such as SAS70 and ISO. Enterprises need to prove compliance with security standards, regardless of the location of the systems required to be in scope of regulation, be that on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources. An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail.

**Securing Data-Storage**

Data protection is the most important security issue in Cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. PaaS based applications, Data-at-rest is the economics of cloud computing and a multitenancy architecture used in SaaS. In other words, data, when stored for use by a cloud-based application or, processed by a cloud-based application, is commingled with other users' data. In cloud computing, data co-location has some significant restrictions. In public and financial services areas involving users and data with different risks. The cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact.

**Patch Management**

The self-service nature of cloud computing may create confusion for patch management efforts. Once an enterprises subscribes to a cloud computing resource—for example by creating a Web server from templates offered by the cloud computing service provider—the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber. Keeping in mind that according to the previously mentioned Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor supplied patches. If patching is impossible or unmanageable, compensating controls such as "virtual patching" need to be considered.

**Conclusion**

One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing. Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. As the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

**References**

1. Kundu A, Banerjee CD, Saha P. Introducing New Services in Cloud Computing Environment, International Journal of Digital Content Technology and its Applications, AICIT. 2010; 4(5):143-152,
2. Lizhe Wang, Jie Tao, Kunze M, Castellanos AC, Kramer

D, Karl W. Scientific Cloud Computing: Early Definition and Experience, 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep, 2008; ISBN: 978-0-7695-3352-0.

3. Grossman RL. The Case for Cloud Computing," IT Professional. 2009; 11(2):23-27, ISSN: 1520-9202.
4. Kandukuri BR, Paturi R, Rakshit VA. Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing. 2009; 517-520.
5. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009). 2009,109-116.
6. Websites
7. British Standards Institution
8. Communications-Electronics Security Group
9. Internet Assigned Numbers Authority